Projeto - computação em nuvem

Objetivo: O desenvolvimento de uma infraestrutura de servidores, fazendo o uso de contêineres e virtualização em Linux. Serão aplicadas neste projeto, as quatro camadas de segurança (controle de acesso, segurança interna, monitoramento, recuperação e disponibilidade do sistema). A tarefa deste servidor, será a de hospedagem de sites e sistemas. Este servidor também fará uso dos princípios e diretrizes da ISO9001 (gestão de qualidade dos produtos e serviços) para a implementação e documentação do mesmo.

Principais diretrizes da ISO9001 a serem implementadas na gerência do projeto:

ISO 9001, será usada para a documentação e implementação. Essa ISO é baseada no controle de gestão de qualidade de produtos e serviços. Seus principais benefícios, tópicos e objetivos que estarão abordados nesse projeto, será o aumento da confiabilidade e melhoria contínua dos processos, produtos e serviços.
Assim como os benefícios de fazer a utilização dessa ISO, teremos também como principal objetivo os seguintes tópicos:

- Liderança;
- Abordagem do processo;
- Melhoria contínua;
- Tomada de decisão baseada em evidências.

Requisitos necessários para implementação do sistema:

- Tipo de servidor: Armazenamento de sites
- Sistema operacional: Debian
- Software de virtualização: VirtualBox
- Contêineres: docker
- Ferramenta de monitoramento: Zabbix e Proxmox
- Redes: Roteadores, switches, firewalls

Requisitos do hardware

- Processador(CPU): Um processador multi-core é recomendado para lidar com múltiplas tarefas

simultaneamente.
- Memória RAM: 4-8GB.
- Armazenamento: São preferíveis SSD. A capacidade depende do volume de dados do servidor.
- Rede: 10Gbps.
- Fonte de alimentação: Fonte de alimentação redundante.

Requisitos de software:

- Distribuição Linux a ser utilizada: Debian

Monitoramento e gerenciamento de redes:

O papel crucial do administrador de redes é ser responsável por inspecionar e garantir que a
infraestrutura de uma rede de computadores permaneça estável. Os principais papeis do gerencimento da rede são:

- Monitoramento de rede: processo contínuo de revisão e análise do desempenho infraestrutura de rede, sendo de grande importância para a detecção precoce de ameaças de segurança, evitando potenciais interrupções ou violações de dados, bem como a melhora significativa de economias de tempo e recursos.
- Gerenciamento de segurança: Proteger a rede de possíveis ameaças tanto externas(Ramsomware, DDos, trojans) quanto internas (ex-funcionário, pessoas com acesso à rede).
- Manutenções e suporte: fornecer suporte para usuários e solucionar possivéis erros de conectividades.

Configuração de servidores

Um servidor é um computador ou sistema de computadores que armazena, processa e fornece acesso a recursos, como arquivos, páginas da web, aplicativos e serviços, para outros computadores ou dispositivos conectados em uma rede.
Os principais elementos para a configuração de servidores são: sistema operacional, servidor web, banco de dados, firewall e segurança, cache e otimização de desempenho.

Gerenciamento de virtualização

O gerenciamento de virtualização é o processo de usar software para administrar e otimizar ambientes virtualizados. Isso envolve a criação, monitoramento e manutenção de máquinas virtuais (VMs) e a alocação eficiente de recursos de hardware físico subjacente.
Principais funções do gerenciamento de virtualização:

- Provisionamento: Criação e configuração de novas máquinas virtuais conforme necessário.
- Monitoramento: Acompanhamento do desempenho e da utilização dos recursos das VMs.
- Conformidade: Garantia de que as VMs estão seguras e em conformidade com as políticas de TI.
- Operações: Manutenção e otimização contínua dos recursos virtuais e físicos

Recursos necessários para implementação de infraestrutura com o Docker

Introdução:

O que é o Docker?

O Docker é uma plataforma de software que permite criar, implantar e gerenciar aplicativos em contêineres. Um contêiner é uma unidade padronizada de software que empacota o código da aplicação e todas as suas dependências, como bibliotecas e ferramentas do sistema, garantindo que o aplicativo funcione de maneira adequada em qualquer ambiente.

Por que o Docker?

1. **Leveza e eficiência:** Diferentemente das máquinas virtuais (VMs), que virtualizam um sistema operacional completo, os contêineres Docker compartilham o kernel do sistema operacional do host, tornando-os mais leves e rápidos para iniciar.
2. **Portabilidade:** Os contêineres Docker podem ser excluídos em qualquer ambiente de suporte Docker, seja laptop, em servidores locais ou na nuvem. Isso facilita a movimentação de aplicativos entre diferentes ambientes sem a necessidade de reconfiguração.
3. **Consistência:** Com Docker, você pode garantir que o seu aplicativo funcione da mesma forma em desenvolvimento, teste e produção, eliminando problemas de “funcionamento da minha máquina”.
4. **Escalabilidade:** Docker facilita a escalabilidade de aplicativos, permitindo que você crie e gerencie clusters de contêineres com ferramentas como Docker

Swarm ou Kubernetes.

Por que utilizar o Docker em uma máquina virtual?

1. **Isolamento Adicional:** Executar Docker dentro de uma máquina virtual adiciona uma camada extra de isolamento, o que acaba por ser útil para aumentar a segurança.
2. **Compatibilidade:** A máquina virtual faz com que o host não tenha a necessidade de trocar o sistema operacional para cada aplicação específica.
3. **Ambientes de Desenvolvimento:** É comum se utilizar de Vms para simular diferentes sistemas operacionais. O Docker pode ser usado dentro dessas VMs para garantir que os aplicativos sejam compatíveis e portáveis.

Requisitos de hardware:

CPU

Uma CPU com suporte à virtualização (VT-x/AMD-V) é essencial para executar máquinas virtuais de forma eficiente, melhorando o desempenho e o isolamento. CPUs multi-core permitem a execução simultânea de múltiplos contêineres Docker, distribuindo a carga de trabalho e garantindo que cada contêiner tenha os recursos necessários. Quanto mais contêineres você planeja executar, mais núcleos são necessários para manter o desempenho ideal.

Memória RAM

A quantidade de RAM disponível impacta diretamente o desempenho dos contêineres Docker. Cada contêiner consome uma parte da memória para executar seus processos e serviços. Se a RAM for insuficiente, o sistema pode começar a usar memória swap, o que reduz significantemente o desempenho. Quanto mais contêineres e serviços você planeja executar, maior será a necessidade de RAM para garantir que todos funcionem de maneira eficiente e sem interrupções. A falta de RAM pode levar a lentidão, falhas e até a paralisação total do sistema.

Rede

Uma boa conectividade de rede é indispensável para o desempenho eficiente dos contêineres Docker. Para começar, o download de imagens Docker requer uma conexão rápida e estável para evitar atrasos e falhas na transferência de dados. Além disso, a comunicação entre contêineres, especialmente em arquiteturas de micros serviços, depende de uma rede confiável para assegurar a troca rápida de informações. Problemas de conectividade podem levar a alta latência, perda de pacotes e interrupções na comunicação, atrapalhando a performance geral dos aplicativos. Portanto, uma infraestrutura de rede robusta é crucial para manter a eficiência, a segurança e a escalabilidade dos sistemas baseados em contêineres.

Requisitos de software:

Sistema operacional
O Docker é amplamente suportado em várias distribuições Linux. Sendo as três com melhor compatibilidade: **Ubuntu, Debian e CentOS.**

Dependências e Pacotes necessários
De maneira prévia a instalação do Docker, alguns pacotes são necessários para instalar e configurar os contêineres Docker. Sendo eles:
• **curl:** Para transferir dados com URLs;
• **ca-certificates:** Para garantir conexões seguras;
• **apt-trasporte-https:** Permite que o APT use repositórios via HTTPS;
• **software-properties-common:** Adiciona scripts de gerenciamento de repositórios;
• **gnupgn:** Ferramentas para criptografia e gerenciamento de chaves.

Docker engine
O Docker Engine é o componente principal que permite a criação e execução de contêineres Docker. Existem **duas** versões principais do Docker Engine: **Community Edition (CE)** e **Enterprise Edition (EE)**. A escolhida pela equipe foi a versão Community Edition (CE).

Docker Engine – Community Edition (CE)
• **Gratuito e Open Source:** Ideal para desenvolvedores individuais, pequenas equipes e projetos de código aberto;
• **Ampla Comunidade de Suporte:** Grande base de usuários e desenvolvedores que contribuem com documentação, tutorias e suporte comunitário;
• **Flexibilidade:** Adequado para ambientes de desenvolvimento, testes e pequenas implementações em produção.

Vantagens do uso de redes distribuídas:

A integração dos serviços em uma rede distribuída envolvem a interconexão de vários "nós" ou sistemas que trabalham juntos para fornecer serviços de forma eficiente e resiliente. Em uma rede distribuída, não há um ponto central de controle; em vez disso, cada nó pode operar de forma independente, mas colaborativa.
Vantagens das redes distribuídas:

- Resiliência: Se um nó falhar, os outros podem continuar operando normalmente, garantindo maior disponibilidade do serviço
- Escalabilidade: É possível adicionar novos nós à rede sem grandes dificuldades, permitindo que a rede cresça conforme necessário.

- Eficiência: A carga de trabalho pode ser distribuída entre os nós, otimizando o desempenho e reduzindo o tempo de resposta.

Recursos necessários para controle das camadas de segurança e monitoramento:

As quatro camadas de segurança.

Com base em estudos realizados durante o desenvolvimento deste trabalho, o autor desta monografia definiu quatro camadas de segurança, que são:

- controle de acesso ao sistema;
- segurança interna do sistema;
- monitoramento do sistema;
- recuperação e disponibilidade do sistema.
  A escolha destas quatro camadas foi baseada nas técnicas e tecnologias hoje empregadas para prover segurança, e nas ações mais comuns que um atacante executa ao tentar invadir um sistema.

Controle de acesso ao sistema: essa camada de baseia no fato de que um atacante precisa monitorar o trafego da rede ou do sistema para obter informações sobre seu funcionamento, para isso, primeiro o atacante precisa obter acesso ao sistema/rede, seja com engenharia social, furto de senhas, sniffers, entre outros.
Ao obter acesso ao sistema, o atacante pode explorar vulnerabilidades nas configurações internas do mesmo, isto é, procurar brechas que o permitam realizar o próximo passo de sua invasão, que é a alteração, exclusão ou furto de arquivos do sistema, em casos mais graves já foram realizadas formatações completas do sistema.

recuperação e disponibilidade do sistema: aproveitando o gancho, em casos de ataques bem sucedidos onde o atacante consegue furtar, alterar, excluir ou formatar o sistema, se faz necessário um plano de recuperação para a manutenção da disponibilidade do sistema, note que a disponibilidade é um fator que consta nos três pilares da segurança da informação. Planos de backup, métodos seguros de armazenamento de backup e até mesmo períodos de backup são itens a serem verificados nessa camada da segurança.

monitoramento do sistema: a camada de monitoramento do sistema se trata da constante verificação do desempenho do sistema, bem como de seus serviços, desempenho, e integridade, a fim de proporcionar a prevenção de ataques além da implementação de atualizações quando necessárias, isto também torna mais fácil a utilização dos backup do sistema, uma vez que o monitoramento de seu status e desempenho podem ajudar a identificar o que foi perdido.

Segurança interna: a camada de segurança interna e a camada de controle de acesso interagem entre si, de modo a complementarem o seu funcionamento, o controle de acesso

dos funcionários ao sistema e rede pode ser visto como uma segurança interna, o controle de funcionamento dos hosts internos da empresa e de suas dependências também, a má configuração de um serviço e a falta de instrução dos usuários que estão utilizando o mesmo podem gerar brechas permitindo o acesso de hackers no mesmo outro item que pode ser avaliado como incluso na segurança interna é o controle da implementação de atualizações do sistema, tanto para mais quanto para menos, atualizações devem ser feitas com cautela para que não afete o funcionamento do servidor.

Cada camada tem uma função e objetivo. A camada de controle de acesso ao sistema trata das interações dos usuários, dispositivos ou aplicativos durante o acesso ao sistema. Para aumentar a segurança de um sistema, apenas os usuários autenticados, devem ter acesso somente às portas e protocolos autorizados em um determinado servidor. A segunda camada trata da segurança interna do sistema. Um sistema torna-se mais seguro quando os seus componentes são atualizados e configurados corretamente conforme documentação oficial do desenvolvedor. Apenas os componentes realmente necessários devem ser adicionados ao sistema. Outro ponto importante é definir permissões restritivas no sistema de arquivos e usar criptografia para proteger arquivos ou diretórios, ou para proteger as comunicações de rede. A camada monitoramento do sistema, trata das técnicas e tecnologias utilizadas para monitorar os componentes do sistema. O monitoramento do sistema pode ser realizado através do monitoramento de registro de eventos, ferramentas específicas de monitoramento e verificação de integridade, ou scripts. O monitoramento do sistema permite que sejam monitorados os componentes de hardware e software do computador. Em um sistema medianamente seguro, uma invasão irá exigir esforço e tempo, de forma que, com um monitoramento eficiente, a invasão pode ser bloqueada em seu início. A camada de recuperação e disponibilidade do sistema, trata das técnicas e tecnologias utilizadas para garantir a recuperação do sistemas e dos dados após um desastre, e para aumentar a disponibilidade do sistema. Um procedimento de contingência bastante utilizado para recuperação é a realização de backups.
Entre as tecnologias empregadas para aumentar a disponibilidade de um sistema, estão, a utilização de clusters, storages e RAID de discos